

# Sigma Rules & Conversion







title: #Title of your rule

id: #Universally Unique Identifier (UUID) Generate

one from https://www.uuidgenerator.net

status: #stage of your rule testing

description: #Details about the detection

intensions of the rule.

author: #Who wrote the rule.

date: #When was the rule written.
modified: #When was it updated

logsource:

**→category:** #Classification of the log data for

detection

→ product: #Source of the log data

detection:

**→**selection:

→→ FieldName1: #Search identifiers for the detection

→→FieldName2:

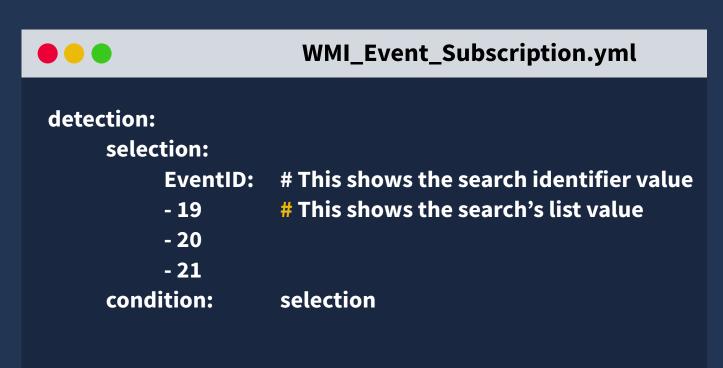
→ condition: #Action to be taken.

**fields:** #List of associated fields that are important for the detection

**falsepositives:** #Any possible false positives that could trigger the rule.

**level:** medium #Severity level of the detection rule.

### **Detection Expression**



#### General Detection Expression Principles

Adapted from: https://github.com/SigmaHQ/sigma/wiki/Specification

- YAML rules apply
- All values are case-insensitive strings with wildcards: '\*' and '?'
- Wildcards can be escaped with \,e.g.\\*. If a wild-card after a backslash should be searched, the backslash has to be escaped: \\\*
- Empty value: ''
- Null value is defined with 'null'

# **Condition Expression**





Operator	Example
Logical and/or	Selection1 or selection2
1/all of search-identifier	1 of selection
1/all of them	All of them
1/all of search-id-pattern	All of filter_*
Negation with 'not'	Selection and not filter
Order of operation '()'	1 of selection andnot (filter1 or filter2)

Data Type	Example	Operator
Lists	EventID: - 4605 - 8201	OR
Maps	Filter: EventID: 3325 EventID: 4523	AND

Value Modifier	What it Does Example	Example
contains	adds a * to the beginning & end of the field value	'CommandLine   contains'
all	Changes the default list behavior from "or" to "and"	CommandLine   contains   all
startswith	Adds a * to the end of the field value	Image   startswith
endswith	Adds a * to the beginning of the field value	Parentimage   endswith
re	Allows the use of Regex	Hostname   re: '^[A-Za-z0-9]{16}\$'

## Sigma Rule Conversion

user@THM\$ /sigma/tools/sigmac -t qradar rules/windows/process\_creation\_win\_anydesk.yml

SELECT UTF8(payload) as search\_payload from events where ((EventID='1' and LOGSOURCETYPENAME(devicetype) ilike '%Microsoft Windows Security Event Log%') and (Description='AnyDesk' or Product='AnyDesk' or Company='AnyDesk Software GmbH'))

user@THM\$ /sigma/tools/sigmac -t splunk -c sysmon rules/windows/process\_creation\_win\_anydesk.yml

(EventID:"1" (Description="AnyDesk" OR Product="AnyDesk" OR Company="AnyDesk Software GmbH"))

user@THM\$ /sigma/tools/sigmac -t es-qs -c winlogbeat rules/windows/process\_creation\_win\_anydesk.yml

(winlog.event\_data.Description:"AnyDesk" OR winlog.event\_data.Product:"AnyDesk" OR winlog.even\_data.Com-pany:"AnyDesk\Software\GmbH")